CONSULTA Y RESPUESTAS 19/09/2025

PREGUNTA 1 LICITDORA. En el PPT del Lote 2 se indica que el servicio deberá contar con un sistema de Detección y Respuesta Avanzada (XDR) que permita identificar patrones sospechosos, clasificar y detectar amenazas complejas, así como generar informes y recomendaciones automatizadas. Pregunta:

¿Debe entenderse que el adjudicatario está obligado a proporcionar la solución tecnológica de XDR como parte del servicio, o bien VEIASA pondrá a disposición esta herramienta y el adjudicatario únicamente deberá operarla?

En caso de tener que proporcionar la herramienta ¿Podrían establecer el número de Endpoint?

RESPUESTA: El ofertante debe proporcionar la solución tecnológica de XDR como parte del servicio. En caso de que esta solución requiriera la instalación de agentes en endpoints, el número aproximado de endpoints sería de 400.

PREGUNTA 2 LICITDORA.. En los criterios de valoración se otorgan 2 puntos por disponer del nivel máximo de partner del fabricante de la solución SIEM. Entendemos que dicho nivel está fundamentalmente asociado a volumen de negocio con el fabricante, y no refleja necesariamente la capacidad técnica del licitador. Pregunta:

¿Podrían admitir puntuación equivalente cuando, aun teniendo un nivel de partner inferior, el licitador acredite capacidad técnica mediante:

1. Certificaciones oficiales del producto SIEM en el equipo de trabajo.

2. Acreditación como MSSP o acuerdo vigente de contrato para la distribución del producto en formato servicio con el fabricante del SIEM.

RESPUESTA:

No. Disponer de nivel máximo de partner del fabricante proporciona beneficios a las empresas, que repercuten positivamente en la calidad del servicio que estas ofrecen.

PREGUNTA 3 LICITDORA.. Si la combinación de capacidades del SIEM y del SOAR, permite ejecutar acciones de respuesta automatizadas incluso cuando el agente EDR del endpoint no está operativo. Entre otras, aislamiento de host por red, finalización de procesos, revocación de sesiones y tokens, bloqueos de IoC (hash/IP/dominio) en controles perimetrales, ejecución de scripts de remediación y políticas de acceso condicional, ¿Puede considerarse esta capacidad funcional equivalente como cumplimiento del criterio “EDR nativo” a efectos de puntuación en el Lote 2?

RESPUESTA: Sí, siempre que se acredite suficientemente que los sistemas de respuesta automática ante incidentes puedan actuar como EDR de un endpoint en los casos concretos en los que el EDR propio del endpoint no esté operativo.

PREGUNTA 4 LICITDORA.. En relación al Lote 2, ¿puede considerarse cumplido el requisito de “Tier III ” cuando se acredite que aunque no se tenga la certificación se cumplen o superan las medidas exigidas para un Data Center Tier III?

RESPUESTA: No. Como parte de los criterios de solvencia técnica y profesional del Lote 2 se exige la certificación o demostración de que se cumplen las medidas de la norma 22301 sobre continuidad de los servicios en caso de que se produzca un problema que afecte a su disponibilidad.
Aportar la certificación TIER III se puntúa adicionalmente como forma de asegurar que la infraestructura que da soporte a los servicios que se solicitan ofrece una alta disponibilidad, minimizando el riesgo de que estos servicios se vean interrumpidos.